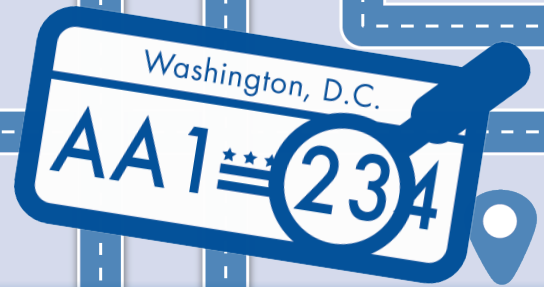




NACDL
FOURTH
AMENDMENT
CENTER



ALPR Primer

What is an ALPR? An automated license plate reader (ALPR) pairs high-speed cameras with image-processing software to identify vehicles and pinpoint their location.¹ ALPR software can run on a wide range of fixed and mobile cameras, including those mounted on streetlights and highway overpasses, affixed to police vehicles or trailers, or paired with police dashcams and mobile phones through an app-based interface.² The images or videos collected usually capture the license plate, which is converted into machine-readable text, as well as a substantial part of the vehicle which can include the make, model, occupants, and immediate vicinity.³ These images and license plate text are paired with information on the date, time, and GPS location of where the vehicle was detected (together, “license plate data”).⁴

How is the data stored? Because ALPR systems capture license plate data of all vehicles scanned, not just of those associated with investigations, database entries can number in the billions.⁵ These databases may be maintained by individual government agencies, pooled together into regional sharing systems, or aggregated by private companies from a variety of sources and accessed via subscription.⁶ Data retention varies across jurisdictions; agencies may retain the collected data for weeks, months or even years.⁷

How is the data used? ALPR systems generally produce two types of data — real-time alerts and historical data. Real-time alerts notify law enforcement officers when a license plate that is enrolled on a watchlist is detected, identifying the current location of the vehicle.⁸ Historical data is generated by searching an ALPR database for specific vehicle data, returning all instances when that plate was detected and producing a map of where that vehicle has been over a set time-period.⁹ Most ALPR systems are searchable by whole or partial plate or particulars about a given vehicle such as make, model, color, and location sighted if the license plate is unknown.¹⁰ Both real-time and historical ALPR data can also be used to “geofence” an area of interest such as a building under investigation, a crime scene, or a widely-attended rally, triggering vehicle monitoring of a specified geographic location live or for post-event analysis.¹¹

ALPR companies advertise predictive or other analytical capabilities as well, including: determining likely future vehicle movement and location based on past patterns;¹² “convoy analysis” or data about which vehicles appear to travel together or be otherwise associated;¹³ automated flags or database queries based on “patterns of behavior” such as plate capture in a particular location deemed to be unusually frequent or anomalous;¹⁴ and pairing ALPR information with other surveillance or investigative systems such as gunshot detection.¹⁵

Potential legal arguments.

Courts in several jurisdictions have considered whether law enforcement use of ALPRs for historical or real-time location tracking would require a warrant under the Supreme Court’s holding in *Carpenter v. United States*, 138 S. Ct. 2206 (2018).¹⁶ Like the historical cell-site location information data in *Carpenter*, ALPR systems give the government access to information that would be “otherwise unknowable” without the use of technology.¹⁷ Many courts have suggested that ALPR location tracking *may* rise to the level of intrusion found in *Carpenter* and thus need a warrant; none, however, have yet found this threshold to be met by the tracking in question.¹⁸ This leaves the door open for a fact-specific argument that the large-scale use of ALPRs to track and locate a vehicle without a warrant could violate the Fourth Amendment and require a suppression remedy. The following recommendations will assist in determining whether it is appropriate to bring such a challenge:

1. Discovery. If it is unclear how law enforcement ascertained the location of a vehicle in your case, consider making detailed requests in discovery for information on ALPR use, as well as motions to compel if necessary.

- The size and scope of the ALPR system, including number of cameras, length of time the data is retained, and how many scans are stored within a database will be material to determining whether a reasonable expectation of privacy was exceeded by the scope of the system or search.¹⁹
- Information about whether the ALPR database is created, owned, and operated by a private company rather than a public agency may trigger third-party doctrine treatment and arguments regarding the “inescapable and automatic nature” of ALPR data collection.²⁰
- The search capabilities of the specific ALPR software used, such as an agency’s ability to conduct searches for “patterns of behavior,” “convoy analysis” or other advanced searches may be instrumental in identifying unique use cases that may amount to suspicionless searches.
- Information about the type and model of the cameras that produced the plate scans may be relevant in determining the accuracy of the scan and whether the requisite level of suspicion required for adverse action to be taken was met.²¹
- State laws or regulations may require an agency to create policies, audit logs, or other discoverable documents.²²

2. Suppression. A motion to suppress ALPR evidence may be supported by the following arguments:

- **Location tracking without a warrant.** ALPR-based location tracking may invoke Fourth Amendment protections. In *Commonwealth v. McCarthy*, 484 Mass. 493 (2020), the court reasoned that: “With enough cameras in enough locations, the historic location data from an ALPR system in Massachusetts would invade a reasonable expectation of privacy and would constitute a search for constitutional purposes. The one-year retention period ... certainly is long enough to warrant constitutional protection.”²³
- **Absence of suspicion for the search.** A search of an ALPR database is likely a search of millions of people’s location and related data over a period of weeks, months, or years. ALPR database searches for “patterns of behavior” may especially lack particularized suspicion of wrongdoing to initiate a search. These searches require an officer to: a) assume a driving pattern is indicative of criminal activity, such as multiple “hits” near a sensitive location indicating a credible security threat or short trips between particular locations being consistent with narcotics trafficking; and b) then search the driving patterns of every person in the database for a match to that behavior. Defense counsel may also consider arguing that in addition to the query, license plate data collection also constitutes a search.²⁴
- **Implicates the First Amendment.** The use of ALPRs to track a person’s movements or obtain information about a person’s associations with other individuals, locations, or events may implicate First Amendment protections. One ALPR vendor, for example, described the real-world use of its product to monitor a motorcycle gang rally in 2018 “to gather data ... should events occur during the rally that would require investigating.”²⁵ When searches implicate First Amendment concerns, courts may look for Fourth Amendment requirements to be followed with “scrupulous exactitude.”²⁶
- **Insufficient grounds for an investigatory detention.** An ALPR alert alone may be insufficient grounds on which to stop a vehicle. Officers may be required, by statute or otherwise, to take additional steps to verify that the ALPR produced an accurate scan.²⁷



3. Admissibility. The admissibility of advanced technology and the testimony accompanying its findings is generally governed by either the *Frye* or *Daubert* standard.²⁸ The Supreme Court's holding in *Daubert* may require ALPR systems — particularly if their predictive or other analytical capabilities are used — be subject to scientifically valid testing and verification prior to use as evidence in court.²⁹

4. State law. Several states have passed laws governing police ALPR use and data retention.³⁰ Check the fact pattern of your case against any relevant state laws for agency requirements and inconsistencies such as law enforcement use of a system restricted to tolling or ALPR data retained or accessed in violation of legislative requirements.

Additional Resources

- *Automated License Plate Readers: State Statutes*, Nat'l Conf. of State Legislators (2022), <https://www.ncsl.org/technology-and-communication/automated-license-plate-readers-state-statutes>.
- Ángel Díaz & Rachel Levinson-Waldman, *Automatic License Plate Readers: Legal Status and Policy Recommendations for Law Enforcement Use*, Brennan Center (2020), <https://www.brennancenter.org/our-work/research-reports/automatic-license-plate-readers-legal-status-and-policy-recommendations>.
- *Commonwealth v. McCarthy*, 484 Mass. 493 (2020), <https://law.justia.com/cases/massachusetts/supreme-court/2020/sjc-12750.html>.
- Christopher Slobogin and Sarah Brayne, *Surveillance Technologies and Constitutional Law*, Annual Review of Criminology (2023), <https://www.annualreviews.org/doi/pdf/10.1146/annurev-criminol-030421-035102>.

Notes

1. See *Automated License Plate Reader (ALPR)*, DEPT. OF HOMELAND SECURITY (Jan. 2021), https://www.dhs.gov/sites/default/files/publications/2021_st_alprfactsheet_20210105_final508.pdf. ALPRs are also sometimes referred to as License Plate Readers, Automatic Vehicle Identification, Car Plate Recognition, and License Plate Recognition.
2. See, e.g., *Selecting the Right License Plate Recognition Solution for Your Agency: A Comprehensive Guide to Building a Successful LPR Program*, MOTOROLA SOLUTIONS, available at <https://app.hushly.com/runtime/content/NnrVf8WY0nRuHXkT>, describing six types of ALPR camera deployments: fixed, quick-deploy, video-based, trailer, mobile dash-cam, and app-based, (last visited July 7, 2023).
3. Some systems additionally capture accelerometer data for the purposes of enforcing speed limits. See, e.g., *ALPR: Automatic license plate recognition*, JENOPTIK, <https://www.jenoptik.us/products/civil-security/alpr> (last visited July 7, 2023).
4. See *Commonwealth v. McCarthy*, 484 Mass. 493, 494 (2020) (describing the data collected by an ALPR system); see *Automated License Plate Readers (ALPRs)*, EFF, <https://www.eff.org/pages/automated-license-plate-readers-alpr> (last visited July 7, 2023).
5. Motorola Solutions, for example, advertises over 44 billion vehicle records on file. *Vigilant VehicleManager Brochure*, 6, MOTOROLA SOLUTIONS, https://www.motorolasolutions.com/content/dam/msi/docs/products/license-plate-recognition-systems/vigilant-vehiclemanager/vigilant_vehiclemanager_brochure.pdf (last visited July 7, 2023). One company, Leonardo ELSAG, advertises the ability to capture up to 1,500 plates per minute. See *License Plate Readers: From Proven Uses to Innovative Deployments*, 1, LEONARDO, <https://www.leonardocompany-us.com/hubfs/LPR/LPR-Product-Sheets/US/Ebook-LPR-Proven-Uses-Innovative-Deployments.pdf> (last visited July 7, 2023).
6. See, e.g., *How LPR Data Can Help Keep Your Community Safer*, 16–19, POLICE1, available at https://www.leonardocompany-us.com/hubfs/LPR/LPR-Product-Sheets/US/Ebook_How-LPR-data-can-help-keep-your-community-safer.pdf (describing the use of ELSAG by the Houston High Intensity Drug Trafficking Area [HIDTA] to collect and share vehicle data from approximately 330 agencies nationwide. Last visited July 7, 2023).
7. In some states this is controlled by law. See, e.g., A.C.A. §§ 12-12-1801–1808 (“Captured plate data ... shall not be used or shared for any other purpose and shall not be preserved for more than one hundred fifty (150) days.”). For a list of state ALPR laws, see *infra* note 30. In many states, however, in the absence of any law or regulation ALPR data retention is set by an individual agency. See, e.g., *License Plate Readers: Impact and Use Policy*, 6, NYPD (Apr. 11, 2021) available at https://www.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/license-plate-readers-lpr-nypd-impact-and-use-policy_4.9.21_final.pdf (“Data collected through NYPD’s LPRs is retained for five (5) years.”).
8. See, e.g., *United States v. Thomas*, 2021 WL 1957412 (5th Cir. 2021) (Officers received an alert that a vehicle suspected to have been stolen had been identified and located at an apartment complex). For restricted areas, plates may also be compared against a “whitelist” of permitted vehicles. See *A Guide to ALPR Recognition Systems*, PROPTIA, available at <https://www.proptia.com/a-guide-to-alpr-recognition-systems/> (last visited July 7, 2023).
9. See 484 Mass. 493 (describing police use of both real-time and historical ALPR data in the police investigation in question).
10. See *supra* note 2 at 12 (The system allows for the user to “set a time frame and proximity to a location, as well as vehicle year, make, model and color parameters, to generate a list of potential vehicles...”). Some systems advertise additional features, such as logging “unique features” of a vehicle like a roof rack, alterations, or stickers. See, e.g., *Flocksafety.com* (last visited July 7, 2023).

11. See *License Plate Readers: From Proven Uses to Innovative Deployments*, *supra* note 5 at 3 (describing the North Texas Sheriff's Criminal Interdiction Unit's use of ALPR trailers "around the event site to gather data (license plate number, photos of each plate on the bike or vehicle, date and time stamps, and trailer identifier). Should events occur during the rally that would require investigating, law enforcement could analyze the data for information to help resolve the issue").
12. Vigilant Solutions, for example, promotes the ability to "use historical vehicle location data to determine potential locations [a person] might be hiding out and when to intercept them." *Vigilant VehicleManager Brochure*, *supra* note 5 at 3. See, e.g., *ELSAG Enterprise Operations Center*, LEONARDO, <https://www.leonardocompany-us.com/lpr/elsag-eoc> (listing "tools for data mining, analysis and monitoring" among its features).
13. See, e.g., *Combat crime with ALPR cameras*, JENOPTIK, <https://www.jenoptik.us/products/civil-security/organized-crime> (promotional video outlining a London case study where ALPR cameras were used to identify and associate two vehicles that passed by Houses of Parliament multiple times over three days, triggering an alert for unusual activity. Last visited July 7, 2023).
14. See *id.* See *supra* note 6 at 18 (describing use of an ALPR system to "see a pattern of life of what they've been doing for as long as we're retaining that data in our database").
15. See, e.g., *Raven*, FLOCK SAFETY, <https://www.flocksafety.com/products/raven> (advertising a system that pairs gunshot detection with license plate readers and video cameras "to deliver real-time, actionable evidence to help officers locate victims, preserve evidence, and identify suspect vehicle leads." Last visited July 7, 2023).
16. See, e.g., 484 Mass. 493; *U.S. v. Bowers*, 2021 WL 4775977 (W.D. Pa. 2021); *U.S. v. Rubin*, 556 F.Supp.3d 1123 (N.D. Cal. 2021); *U.S. v. Graham*, 2022 WL 4132488 (D.N.J. 2022); *State v. Lelyukh*, 2021 WL 5872306 (App. Ct. Minn. 2021). See *Carpenter v. United States*, 138 S. Ct. 2206 (2018).
17. See 138 S. Ct. at 2218.
18. See, e.g., 484 Mass. 493 (2020) (denying a motion to suppress ALPR data and the fruits of the warrantless search on the grounds that "[w]hile the defendant has a constitutionally protected expectation of privacy in the whole of his public movements, an interest which potentially could be implicated by the widespread use of ALPRs, that interest is not invaded by the limited extent and use of ALPR data in this case."); *U.S. v. Bowers*, 2021 WL 4775977 (W.D. PA, 2021) (finding no reasonable expectation of privacy in a license plate because "even in the aggregate, the ALPR cameras' capability to capture multiple shots of a single vehicle and/or store historical data does not approach the near constant surveillance of cell-phone users' public and private movements."); *U.S. v. Yang*, 958 F.3d 851 (9th Cir. 2020) (From Judge Bea's concurrence: "...ALPRs may in time present many of the same issues the Supreme Court highlighted in *Carpenter*. ALPRs can effortlessly, and automatically, create voluminous databases of vehicle location information. If enough data is collected and aggregated, this could have the ability to identify quickly and easily the precise whereabouts and lifestyle habits of those whose vehicle information is recorded. ALPRs also collect information without individualized suspicion, and records can be maintained for years. ").
19. See, e.g., 484 Mass. at 506 (2020) ("The one-year retention period indicated in the [Executive Office of Public Safety and Security] retention policy is certainly long enough to warrant constitutional protection. ").
20. See 138 S. Ct. at 2217 (holding that the fact that information is collected by a third party "does not make it any less deserving of Fourth Amendment protection" given the "depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection. ")
21. See, e.g., *supra* note 2 (describing how certain ALPR solutions, such as the "in-car integrated" camera can experience "difficulties in low-light and with vehicles moving at high speeds, which impact detection and recognition accuracy." Last visited July 7, 2023).
22. See, e.g., Cal. Civ. Code Ann. § 1798.90.51 ("An ALPR operator shall ... implement a usage and privacy policy" to include: "the authorized purposes for using the ALPR system and collecting ALPR information" among other requirements).
23. 494 Mass. at 506. Note the Court ultimately held that there was no invasion of privacy given that the search was limited to a particular license plate and data from four ALPR devices. *Id.* at 509. The duration of the surveillance is material to this inquiry. See 138 S. Ct. at 2215; see also *Leaders of a Beautiful Struggle v. Baltimore Police Department*, 2 F.4th 330, 341 (2021); *United States v. Moalin*, 973 F.3d 977, 991 (9th Cir. 2020); *Klayman v. Obama*, 957 F.Supp.2d 1, 32 (D.D.C. 2013).
24. In determining whether a reasonable expectation of privacy has been invaded, "it is not the amount of data that the [state] seeks to admit in evidence that counts, but, rather, the amount of data that the government collects or to which it gains access." 484 Mass. at 505. See 2 F.4th at 345 (creating a retrospective database of everyone's movements across the city is materially different than single instance of targeted surveillance of an individual suspect or location for a temporary period of time and gives police access to a "category of information otherwise unknowable. ")
25. See *License Plate Readers: From Proven Uses to Innovative Deployments*, *supra* note 5 at 3.
26. See *Stanford v. Texas*, 379 U.S. 476, 485 (1965), see *Zurcher v. Stanford Daily*, 436 U.S. 547 (1978). But see *New York v. P.J. Video*, 475 U.S. 868 (1986) (holding "that an application for a warrant authorizing the seizure of materials presumptively protected by the First Amendment should be evaluated under the same standard of probable cause used to review warrant applications generally."). Some courts have interpreted *P.J. Video* to have abrogated the *Stanford* "scrupulous exactitude" standard. See, e.g., *U.S. v. Perez*, 247 F.Supp.2d 459 (S.D.N.Y. 2003). Many, however, still follow the Supreme Court's holding in *Stanford*. See, e.g., *U.S. v. Nelson*, 847 F.2d 285 (6th Cir. 1988) (noting that "Although in *P.J. Video* ... the Supreme Court ruled that the Fourth Amendment does not require a higher standard of probable cause for warrants authorizing the search for constitutionally protected materials, it left intact *Stanford*'s requirement of a heightened degree of particularity in search warrants."); see, e.g., *U.S. v. Stelten*, 869 F.2d 446 (8th Cir. 1989); see, e.g., *Wabun-Inini v. Sessions*, 900 F.2d 1234 (8th Cir. 1990); see, e.g., *U.S. v. Mayer*, 503 F.3d 740 (9th Cir. 2007); see, e.g., *State v. Roy*, 2019 ME 16 (2019).



27. See *Green v. City & County of San Francisco*, 751 F.3d 1039 (9th Cir. 2014) (“it is disputable whether an officer conducting a stop could reasonably rely on a lack of qualifying information from the [ALPR reading] as a justification for making the stop without an independent verification.”); see *United States v. Esquivel-Rios*, 725 F.3d 1231 (10th Cir. 2013) (emphasizing the importance of the reliability of computer databases in the context of reasonable suspicion for a traffic stop); but see *United States v. Lurry*, 2010 WL 4628178 (W.D. Tenn. 2010) (“the court finds the alert by the ALPR system to be a sufficient basis for the reasonable suspicion necessary to support a Terry stop”), aff’d on other grounds, 483 Fed. Appx. 252 (6th Cir. 2012), and *Hernandez-Lopez v. State*, 319 Ga. App. 662, 663 (Ga. Ct. App. 2013) (“based on the alert and information he received from the LPR system, the officer had reason to believe the male driver of the relevant vehicle was wanted for failure to appear in court, which provided reasonable, articulable suspicion to conduct a traffic stop.”) Some state statutes require visual confirmation of the ALPR alert. See, e.g., N.H. Rev. Stat. § 261:75-b.
28. *Daubert v. Merrell Dow Pharm., Inc.*, 509 U.S. 579 (1993); *Frye v. United States*, 293 F. 1013 (D.C. Cir. 1923).
29. For a more in-depth explanation of this argument, see Christopher Slobogin and Sarah Brayne, *Surveillance Technologies and Constitutional Law*, Annu. Rev. Criminol. 2023, available at <https://www.annualreviews.org/doi/pdf/10.1146/annurev-criminol-030421-035102>.
30. Relevant state statutes include: A.C.A. §§ 12-12-1801–1808 (Arkansas); Cal. Civ. Code Ann. §§ 1798.90.5–55, Cal. Veh. Code Ann. § 2413 (California); C.S.R.A. § 24-72-113 (Colorado); Ga. Code Ann. § 35-1-22, Ga. Code Ann. §§ 40-14-5–6 (Georgia); 29-A M.R.S.A. § 2117-A (Maine); MD Pub. Safety Code § 3-509 (Maryland); M.S.A. §§ 13.824, 626.8472, 13.82 (Minnesota); MCA §§ 46-5-117–118 (Montana); Neb. Rev. Stat. §§ 60-3201–3209 (Nebraska); N.H. Rev. Stat. § 261:75-b (New Hampshire); N.C.G.S.A. §§ 20-183.30–3 (North Carolina); O.R.S. §§ 383.001–55 (Oregon); T.C.A. § 55-10-302 (Tennessee); U.C.A. §§ 41-6a-2001–05 (Utah); 23 V.S.A. § 1607–8 (Vermont); VA Code Ann. § 46.2-819.3:1 (Virginia). Some state regulations also constrain certain ALPR uses. See, e.g., N.H. Code Admin. R. Saf-C 7203.01 (New Hampshire); 290-RICR-60-00-2.4 (Rhode Island). Some additional states not listed above exempt ALPR data from public records disclosure. See, e.g., F.S.A. §§ 316.0777–8 (Florida); K.S.A. §§ 45-217–22 (Kansas, includes location of ALPR devices as exempt from disclosure).

About the National Association of Criminal Defense Lawyers (NACDL)

The National Association of Criminal Defense Lawyers (NACDL) envisions a society where all individuals receive fair, rational, and humane treatment within the criminal legal system.

NACDL’s mission is to serve as a leader, alongside diverse coalitions, in identifying and reforming flaws and inequities in the criminal legal system, and redressing systemic racism, and ensuring that its members and others in the criminal defense bar are fully equipped to serve all accused persons at the highest level.

About the Fourth Amendment Center

NACDL’s Fourth Amendment Center offers direct assistance to defense lawyers handling cases involving new surveillance tools, technologies and tactics that infringe on the constitutional rights of people in America.

The Center is available to help members of the defense bar in bringing new Fourth Amendment challenges.

To request assistance or additional information, contact 4AC@nacd.org.

How to Support Our Work

You can support our mission and enhance your career by becoming a member of the NACDL. Learn more by visiting

<https://www.nacd.org/Landing/JoinNow>.



NACDL FOURTH
AMENDMENT CENTER

For litigation assistance and other resources contact 4AC@nacd.org